

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK**

AMERICAN FEDERATION OF GOVERNMENT
EMPLOYEES, AFL-CIO, *et al.*,

Plaintiffs,

v.

U.S. OFFICE OF PERSONNEL MANAGEMENT, *et al.*,

Defendants.

Case No. 1:25-cv-01237-DLC

**DECLARATION OF BRUCE SCHNEIER IN SUPPORT OF
PLAINTIFFS' MOTION FOR PRELIMINARY INJUNCTION**

I, Bruce Schneier, declare as follows:

1. I am over eighteen years of age and competent to give this declaration. This declaration is based on my personal knowledge, information, and belief.

2. I have been a security technologist for more than thirty years, focusing on all aspects of cybersecurity. I am currently an adjunct lecturer at the Harvard Kennedy School, where I teach cybersecurity policy. I am a fellow at the Belfer Center for Science and International Affairs, the Ash Center for Democratic Governance in and Innovation, and the Berkman Klein Center for Internet and Society—all at Harvard University. I am the author of more than a dozen books and hundreds of articles, essays, and papers on digital security and cybersecurity. I have testified before Congress, served on government committees, and am a frequent commentator about security and privacy issues. I am a Board Member of the Electronic Frontier Foundation and AccessNow, and an Advisory Board Member of the Electronic Privacy

Information Center and VerifiedVoting.org. I am also the Chief of Security Architecture at Inrupt, Inc., and a partner at Alchemist Associates LLC.

3. More information about me and links to my many publications about computer and digital security are available at www.schneier.com. My curriculum vitae is attached as Exhibit A.

4. From long experience in this field, I know that engineers and programmers who are skilled in one area of technology are often not skilled at cybersecurity. It requires a different kind of expertise, mindset, and experience to understand and take the appropriate steps to protect computer systems from attack than it does to build or maintain those systems.

5. Based on my experience and the information available on the public record, and as I explain further below, my professional opinion is that imminent risks of significant harm exist for the millions of Americans whose sensitive data is held by the US Office of Personnel Management (OPM), including plaintiffs, as a result of the access to OPM systems given to personnel of the newly created Department of Government Efficiency (DOGE). Additionally, this access has created an imminent risk of harm to America's national security.

6. The longer that people affiliated with DOGE have access to, or copies of, the personnel information in the OPM databases, the more imminent the risk of harm and the greater harm that can occur due to that risk.

7. As I detail further below, the most alarming aspect of the reported activities is that defendants have systematically circumvented security measures that would detect and prevent misuse—including standard incident response protocols, auditing, and change-tracking

mechanisms—in large part by sidelining the career officials in charge of those security measures and replacing them with inexperienced operators.¹

8. The defendants also appear to be operating without proper and experienced oversight, especially with regard to the specific security measures of the many complex systems that OPM operates. The approach and execution of DOGE personnel’s access to OPM systems creates significant security risks and violates longstanding OPM policy.

9. For instance, Declarant Greg Hogan has been at OPM less than four months and was not previously in governmental service. Given that limited experience, his familiarity with OPM systems is likely not deep. Mr. Hogan’s previous experience is with a company owned by Elon Musk that was developing technology to make cars semiautonomous.

10. Additionally, other DOGE engineers obtained access to OPM’s records before the agency confirmed that they had government-issued computers and before they had been vetted in accordance with longstanding agency practices.²

11. In one instance, records were disclosed to an inexperienced engineer who called himself “Big Balls” online, who had previously been fired from a cybersecurity firm following

¹ Letter from Rep. Gerald Connolly, Ranking Member, House Committee on Oversight and Government Reform & Rep. Shontel Brown Ranking Member, House Committee on Oversight and Government Reform, Subcommittee on Cybersecurity, Information Technology, and Government Innovation to Charles Ezell, Acting Director, Office of Personnel Management (Feb. 4, 2025), <https://oversightdemocrats.house.gov/sites/evo-subsites/democrats-oversight.house.gov/files/evo-media-document/2025.02.04.%20GEC%20and%20Brown%20to%20OPM-Ezell-%20DOGE%20Emails.pdf> (Connolly & Brown letter). *See also Tim Reid, Musk aides lock workers out of OPM computer systems, Reuters, Feb. 2, 2025*, <https://www.reuters.com/world/us/musk-aides-lock-government-workers-out-computer-systems-us-agency-sources-say-2025-01-31/>.

² Nick Schwellenbach, *Elon Musk’s DOGE Team Raise Vetting, Ethics Concerns*, Project on Government Oversight, Feb. 6, 2025, <https://www.pogo.org/investigations/elon-musks-doge-teams-raise-vetting-ethics-concerns>; Anthony Kimery, *Internal feud rages over unvetting DOGE access to federal IT systems*, Biometric Update, Feb. 19, 2025, <https://www.biometricupdate.com/202502/internal-feud-rages-over-unvetted-doge-access-to-federal-it-systems>; Charles Rollet, *Federal workers sue Elon Musk and DOGE to cut off data access*, TechCrunch, Feb. 11, 2025, <https://techcrunch.com/2025/02/11/federal-workers-sue-elon-musk-and-doge-to-cut-off-data-access/?guccounter=1>.

(according to a recent firm statement) “an internal investigation into the leaking of proprietary information that coincided with his tenure.”³

12. Reports also indicate that individuals associated with DOGE connected an unauthorized server into the OPM network.⁴

13. As a result of these and other “urgent concerns related to potential unauthorized access of government networks and sensitive information at certain federal agencies, including at the U.S. Office of Personnel Management (OPM)” raised by several members of Congress in a letter dated February 6, 2025, the Office of Inspector General of the OPM initiated an investigation on March 7, 2025.⁵

Types of Security Risks

14. Poor security of OPM’s network creates three distinct kinds of security risks, all of which appear to be present here:

15. **Data exposure.** This is the risk that OPM’s data—both personal information and transaction records—could be accessed or copied.

16. **System manipulation.** This is the risk that, because of poor security, external threat actors could break into OPM’s network. They would be able to manipulate OPM’s systems while also altering audit trails that would provide evidence of their changes. This could include adding and deleting data or installing “backdoors” to facilitate later access.

17. **System control.** This is the risk that external threat actors could fully take control of OPM’s systems. Going beyond mere manipulation, they would be able alter core systems and

³ <https://www.nytimes.com/2025/02/07/us/politics/musk-doge-aides.html>.

⁴ Connolly & Brown Letter.

⁵ <https://oversightdemocrats.house.gov/sites/evo-subsites/democrats-oversight.house.gov/files/evo-media-document/hogr-minority-final.pdf>

authentication mechanisms, while at the same time disabling the very tools designed to detect such changes. This is more than modifying operations; it is modifying the infrastructure that those operations use.

18. These three risks can result in three different types of security breaches: confidentiality, integrity, and availability.

19. **Confidentiality breaches.** These occur when a person's data is exposed. The data OPM has about millions of people is highly personal, and there are many ways to exploit it. External actors who want this data include adversarial foreign state actors like China—who I will discuss further below—and include criminals who want to use the data for identity theft and other forms of fraud.

20. In the case of OPM data, beyond simple exposure of personally identifying information, which is bad enough, the breaches involve unauthorized access to even more sensitive data. This includes personnel security clearance data revealing intelligence connections, background investigation information exposing personal vulnerabilities, financial disclosure forms containing detailed asset information, and medical information revealing conditions that could be exploited.

21. Many of the plaintiffs are at higher risk if their identities and locations are disclosed. This includes those who work undercover or in clandestine government services, as well as the Administrative Law Judges who often face threats of retaliation from litigants.

22. A particular risk for plaintiffs who are targets of foreign intelligence services is that a breach that allows those services to identify intelligence officers can allow these adversaries to build targeting profiles and conduct human intelligence operations against those federal employees.

23. **Integrity breaches** occur when the data is modified, either accidentally or deliberately. Depending on the nature of the modification, this can have catastrophic consequences for plaintiffs, most of whom rely on OPM to receive their proper paychecks, benefits, retirement support, and more.

24. Specifically, unauthorized modifications can allow others to alter security clearance statuses to grant access to unauthorized individuals, modify payroll or benefits information to deny or change benefits in ways that create financial distress, modify employment history in ways that deny or delay promotions or salary increases, insert false disciplinary actions to create grounds for blackmail, or change contact information to intercept communications. These attacks are used by both foreign adversaries and criminals.

25. **Availability breaches** occur when data is deleted or otherwise made unavailable. Any sort of availability breach can be as catastrophic as integrity breaches for people who depend on OPM for their salaries, benefits, and retirement and medical care payments.

26. This kind of breach includes the possibility of ransomware, when an external threat actor encrypts the data and demands payment to unlock it. The criminal ransomware industry is extensive and robust, and countries like North Korea engage in ransomware as a means of funding their government.

27. Unavailable data can result in denial of service, impacting retirement and health benefits and disruption or harm to background investigations.

28. All three of these types of breaches are more likely now that OPM's security is reduced. Indeed, those breaches could already be in process.

Violating Separation of Duties Increases Security Risks

29. Because computer systems like OPMs have such high security requirements, they were designed with the same two-person control principle that guides nuclear launch protocols:

No single person should have the ability to make critical changes to the system. Just as launching a nuclear missile requires two separate officers turning their keys simultaneously, making changes to critical systems that house sensitive personal records traditionally requires multiple authorized personnel working in concert.

30. This approach, known as “two-person control” or “separation of duties,” isn’t just bureaucratic red tape; it’s a fundamental security principle as old as security itself. It is used for many situations, far beyond the nuclear example. When your local bank processes a large transfer, for instance, it requires two different employees to verify the transaction. When a company issues a major financial report, separate teams must review and approve it. These are essential, time-tested safeguards against corruption and error.

31. This principle has been codified in NIST 800-53 AC-5 (Separation of Duties).

32. People associated with DOGE have been granted full administrative access to DOGE systems, which allows them to make changes without the protection provided by a separation of duties protocol.

33. Worse, these same people have been granted and have in fact accessed a wide range of *different* government computer systems across different government agencies, including those of the Defendant Office of Personnel Management,⁶ along with the US Treasury,⁷ the US

⁶ *Elon Musk seizes computer system, locks out senior government officials*, Yahoo, Feb. 2, 2025, <https://www.yahoo.com/tech/elon-musk-seizes-computer-system-171738117.html>.

⁷ *Wyden Demands Answers Following Report of Musk Personnel Seeking Access to Highly Sensitive U.S. Treasury Payments System*, U.S. Senate Committee on Finance, Jan. 31, 2025, <https://www.finance.senate.gov/chairmans-news/wyden-demands-answers-following-report-of-musk-personnel-seeking-access-to-highly-sensitive-us-treasury-payments-system>.

Agency for International Development,⁸ US Citizen and Immigration Services,⁹ and reportedly others. This also violates the security principle of separation of duties.

34. In other words, the same individuals with access to Treasury systems now have access to OPM's personnel database, creating a unified attack surface across multiple critical government functions that can be exploited by adversaries, both foreign and domestic.

35. These reports confirm my fears about a lack of experience and understanding about the security needed for these systems. Both inside and outside of OPM, this kind of broad, uncontrolled access by the same people to multiple systems violates the fundamental separation of duty principles.

Violation of the Principle of Least Privilege Creates Risks.

36. A second principle is known as the Principle of Least Privilege, which holds that a person using a system should only have access to the minimum portion of a system and data necessary to do their jobs and only for as long as they need it.

37. This has been captured in NIST 800-53 AC-6, which lists The Principle of Least Privilege as a key security control.¹⁰

38. In sharp contrast to this Principle, many of the newly hired DOGE personnel, and all of them initially, were granted maximum access to OPM's systems.

39. Federal systems, including OPM, typically implement time-limited, audited privileged access through secure mechanisms like CyberArk/Venafi or BeyondTrust. Reports

⁸ Abigail Williams, et al., *USAID security leaders removed after refusing Elon Musk's DOGE employees access to secure systems*, NBC News, Feb. 2, 2025, <https://www.nbcnews.com/politics/national-security/usaids-security-leaders-removed-refusing-elon-musks-doge-employees-access-rcna190357>.

⁹ (<https://www.theverge.com/policy/643807/doge-uscis-data-naturalization-elon-musk>); <https://www.washingtonpost.com/business/2025/02/10/musk-doge-state-department-surrogate/>

¹⁰ https://csrc.nist.gov/CSRC/media/Projects/risk-management/800-53%20Downloads/800-53r5/SP_800-53_v5_1-derived-OSCAL.pdf

indicate DOGE personnel have obtained persistent administrative access, bypassing these controls. Without proper personnel access management controls, detecting malicious activity becomes nearly impossible, as administrative users can modify audit logs to conceal their actions.

Risks from Hardware or Software Modification

40. Every hardware or software modification to complex systems like OPM's systems normally goes through a complex planning process and includes sophisticated access control mechanisms. The way DOGE has accessed and manipulated the OPM systems has made them much more vulnerable to attack. Making matters worse, as noted above, the experienced, legitimate system administrators trained to protect them have been sidelined, locked out, or driven out.

41. For instance, the Federal Information Security Modernization Act (44 U.S.C. § 3554) requires formal security assessment and authorization before substantive system changes are made.

42. DOGE's reported activities bypass this process, creating unassessed and unauthorized modifications to federal information systems.

Leaving the Door Propped Open

43. Foreign adversaries typically spend years attempting to penetrate government systems such as OPM, using stealth to avoid being seen and carefully hiding any tells or tracks. As the Congressional report on the breach confirms, the Chinese government's 2015 breach of OPM started in 2012, and included the installation of backdoors that were later exploited. The breach was a significant US security failure, and it illustrated how personnel data could be used to identify intelligence officers and compromise national security.

44. By modifying core systems, the DOGE agents have not only compromised current operations but have also likely left behind vulnerabilities that could be exploited in future attacks, giving adversaries such as Russia and China an unprecedented opportunity.¹¹ Those countries have long targeted these government systems, not only to gather intelligence, but to understand how to disrupt these systems in a crisis and to plant backdoors that could be triggered at a later date.¹²

45. This risk, and the irreparable harm that occurred due to the 2015 OPM breach, was identified and discussed in more detail by the House Oversight Committee in its 2016 report, “The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation,”¹³ attached as Exhibit B. It includes an explanation of how the government focused on a first intruder and missed a second one, who later exfiltrated the fingerprints of 5.6 million people.

46. Even more recently, an employee of the National Labor Relations Board provided information to the Senate Select Committee on Intelligence that demonstrated significant

¹¹ Suzanne Smalley, As DOGE teams plug into federal networks, cybersecurity risks could be huge, experts say, *The Record*, Feb. 3, 2025, <https://therecord.media/doge-opm-treasury-cybersecurity>.

¹² PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure, *Cybersecurity Advisory*, Feb. 7, 2024, <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a>; Gintaras Radauskas, China secretly acknowledges Volt Typhoon attacks on US infrastructure: why?, *cybernews*, April 14, 2025, <https://cybernews.com/cybercrime/china-volt-typhoon-infrastructure-taiwan-warning/>; Laila Kerney, US electric grid growing more vulnerable to cyberattacks, regulator says, *Reuters*, April 4, 2024, <https://www.reuters.com/technology/cybersecurity/us-electric-grid-growing-more-vulnerable-cyberattacks-regulator-says-2024-04-04/> (“Geopolitical conflict, including Russia’s invasion of Ukraine and the war in Gaza, have dramatically increased the number of cyber threats to North American power grids, NERC said. Threats also commonly come from China”).

¹³ <https://oversight.house.gov/wp-content/uploads/2016/09/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf>

security problems arising after DOGE was granted access to its systems, including over twenty attempts to access the systems from a Russian IP address.¹⁴

47. The technical details of how these systems operate now, their security protocols, and their vulnerabilities are now potentially exposed to unknown parties without any of the usual safeguards. Instead of having to breach heavily fortified digital walls, these parties can simply walk through doors that are being propped open—and then erase evidence of their actions.

Imminent Harm from DOGE Access

48. If the OPM database has been or will be breached, either due to external attacks made easier through DOGE's activities or mistakes or security failures by the new DOGE team, the consequences would be significant and irreparable.

49. For the plaintiffs, privacy (confidentiality breaches) consequences can include identity theft, fraud, misidentification, harm to credit ratings, stalking, risk of retaliation from foreign adversaries, risk of loss of assets, and vulnerability to blackmail and other forms of exploitation, just to name a few. Any of these can result in substantial harm, loss of money or property, embarrassment, inconvenience, or unfairness. In most data breach situations, people suffer not just one, but many of these harms.

50. For the plaintiffs, integrity consequences can include miscategorization, which can result in a loss of pay, medical care, and other benefits, depending on the data that has been impacted. It can also impact potential promotions, job security, and more.

51. For the plaintiffs, availability consequences can include the same sorts of harms as integrity risks, as well as risks from ransomware and other attacks.

¹⁴ Declaration of Daniel J Berulis, submitted to the Senate Select Committee on Intelligence and the U.S. Office of Special Counsel (April 14, 2025), available at https://whistlebloweraid.org/wp-content/uploads/2025/04/2025_0414_Berulis-Disclosure-with-Exhibits.s.pdf at ¶21.

52. Additionally, as I noted above, OPM's databases contain information about plaintiffs who face particular risks, including two specific kinds.

53. First, it creates more acute risks for current or former government employees who are or have operated under cover or who reasonably fear targeting by a foreign adversary or domestic criminal gang. This category includes many who operate publicly under various pseudonyms for protection of both themselves, their families, and their work.

54. Second, it creates acute risks for government employees in politically charged areas who could receive threats of violence, and face actual violence. For example, Administrative Law Judges often face violence and threats of violence from unhappy litigants. The same is true of employees who interact with the public at various agencies ranging from Social Security to Veterans Affairs to the Internal Revenue Service.

55. There is no indication that defendants have taken any steps to recognize these increased security needs, much less that they have taken any precautions in response of them.

Significance of the 2015 Office of Personnel Management Breach by China

56. As the House Oversight Report (*supra*, note 13) confirms, the 2015 breach exposed 21.5 million records containing SF-86 security clearance forms, which provided detailed information about millions of Americans and their families. Intelligence community sources have confirmed these records were used by Chinese intelligence to identify US intelligence officers operating under nonofficial cover.

57. The direct federal costs exceeded \$500 million for remediation and identity protection services. Individual victims reported spending an average of over 200 hours resolving identity theft issues.

58. The 2015 breach began when attackers obtained legitimate credentials and escalated privileges, which is precisely the vulnerability being recreated by granting DOGE personnel unrestricted access without proper security controls.

59. The American intelligence community continues to deal with the fallout, as the compromised identity/profile data has, in the words of prominent privacy law scholar, Professor Daniel Solove of George Washington University Law School, a harm with “no end.”¹⁵

The Ongoing Risk of Access

60. While any access to OPM’s systems increases the security risks, ongoing access creates ongoing risks. That is because the longer that insecure access of the DOGE actors continues, the greater the chances of any of the breaches discussed above, and therefore any of the harms discussed above, occurring.

61. The risks are immediate, severe, and easily foreseeable, and may have already started happening, even if the consequences are not yet manifest. Quite often, the victims of identity theft and other injuries are not immediately aware of them—the knowledge comes when they receive an incorrect paycheck or benefits payment or are denied benefits entirely. It comes when they are informed of credit problems, billed for services that they did not seek or, worse, arrested or detained based upon incorrect or modified information about them.

62. The consequences for plaintiffs, whose data is now put at increased risk due to DOGE access to the entirety of the data that OPM holds about them, will be difficult if not impossible to fully remedy through money damages. The better option is to curtail any further sharing, and mitigate against the potential for breach by enjoining Defendants from accessing the

¹⁵ <https://www.linkedin.com/pulse/opm-data-breach-harm-without-end-daniel-solove>

data entirely, and taking the other steps I outline below to at least try to block further harms from past access.

63. This is because once the data is taken by others—whether thieves or foreign adversaries—it becomes impossible in any meaningful sense to get it back in a way that entirely prevents or remedies ongoing harm. For instance, if a person suffers one identity theft as a result of the theft of personal data stored in the OPM database, some financial recovery can help but will never fully compensate them for the ongoing loss of the compromised credentials.

64. Additionally, the harm can be ongoing and can be repeated. Once released, the data can be reused multiple times. Similarly, access by one foreign adversary does not mean that another foreign adversary won't gain access via the same or a future breach.

65. This also means that even if the data has not been breached to date, future breaches or attacks are an ongoing risk. This is due to ongoing access by people without sufficient training, experience, oversight, and limitations on use.

66. This also means that even if the data has already been taken by one set of thieves or spies, ongoing access by DOGE risks further attacks and breaches. Put another way, just because plaintiffs may already have been injured by the access and use of their data by Defendants, that does not mean that future, additional harm cannot occur due to continued access and use.

67. In sum, the more people who gain access to their data, and the longer that they have that access, the greater harms plaintiffs face. Preliminary injunctive relief will reduce the future harms plaintiffs may suffer due to DOGE access, even if some harm has already occurred.

DOGE Does Not Need Immediate, Full, and Uncontrolled Access to Personnel Data held by OPM to Fulfill Its Mandate

68. There is a vast difference between actual efforts to carefully and thoughtfully modernize OPM systems, which can be done in a way consistent with the Privacy Act, and what Defendants have done and continue to do.

69. The clearest evidence of this is in the resignation letter of February 25, 2025, from twenty-one members of the former US Digital Service (renamed DOGE) to White House Chief of Staff Susie Wiles.¹⁶

70. These civil servants, who were actually working to modernize many government systems when DOGE took over their renamed agency, noted that the new DOGE agents were “firing technical experts, mishandling sensitive data and breaking critical systems,” in direct contradiction to their stated mission. These civil servants stated, “We will not use our skills as technologists to compromise core government systems, jeopardize Americans’ sensitive data or dismantle critical public services.”

Mitigation Steps

71. As a result of this reckless course of conduct, the Defendants are endangering the very systems they claim to be modernizing, as well as the people who rely on the security and privacy of those systems.

72. To address these vulnerabilities, five immediate steps are essential.

73. **Revoke Access.** DOGE access must be revoked and proper authentication protocols restored. Only after complete vetting and training, and only on an individual basis with a truly justified need, should access be restored, and only based upon the principle of least privilege access.

¹⁶ <https://www.documentcloud.org/documents/25544180-usds-resignation-letter/>

74. **Full Forensic Analysis.** A comprehensive forensic investigation should be conducted to identify all system modifications, data accesses, and potential persistence mechanisms established during the DOGE access period.

75. **Compromise Recovery.** OPM should treat all affected systems as potentially compromised, consistent with a Cyber Incident Response Plan in accordance with NIST SP 800-61r2.


76. **Clean System Rebuild.** Critical authentication and authorization systems should be rebuilt from trusted media on clean hardware.

77. **Independent Security Assessment.** An independent security assessment should be conducted by qualified third-party experts (not affiliated with DOGE) to validate the effectiveness of remediation efforts.

78. Each day of continued unrestricted access makes the eventual recovery more difficult and increases the risk of irreversible damage to these critical systems and to the people whose data is stored in them. While the full impact may take time to assess, these steps represent the minimum necessary actions to begin restoring system integrity and security protocols.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on April 24, 2025.



Bruce Schneier